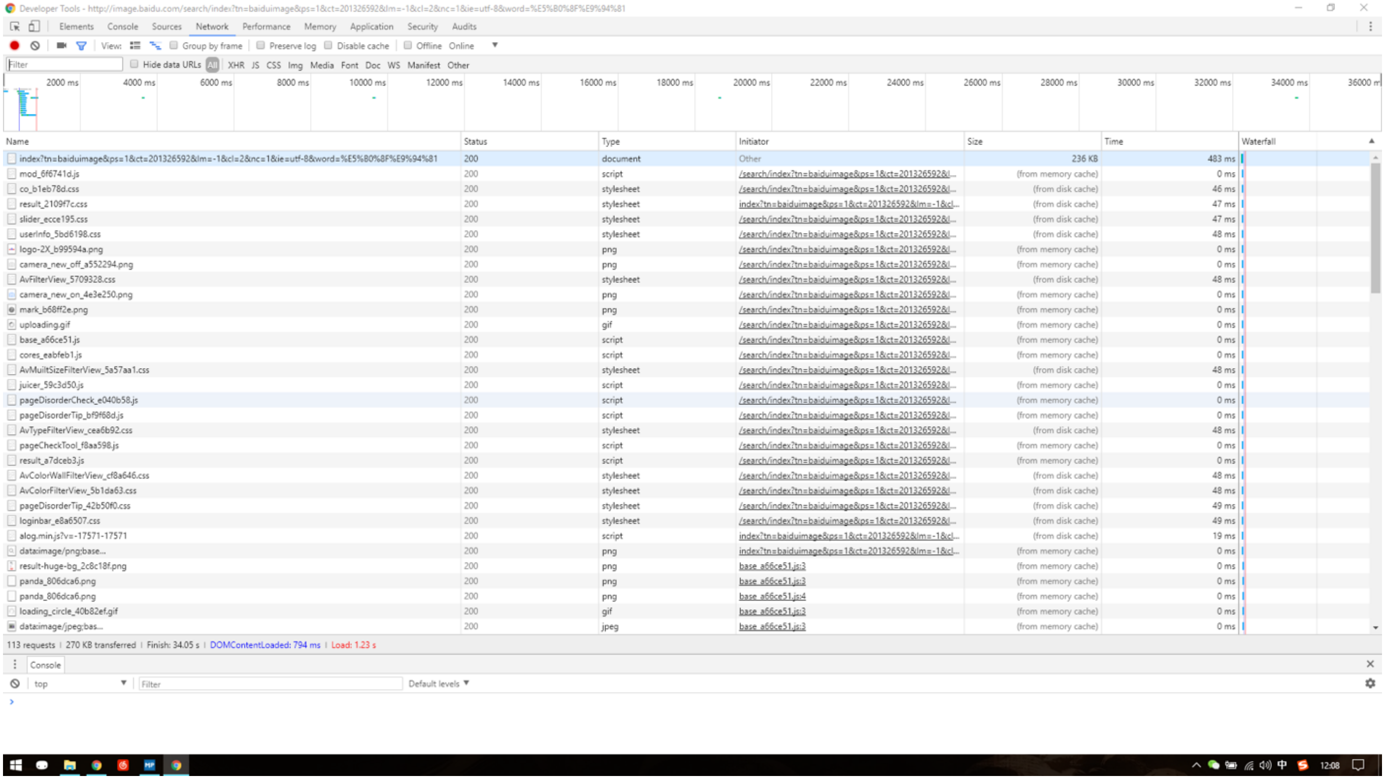
【13】第六章 | 下载前必须了解到的安全，监控和法律问题

平时在下载文件的时候，我们不仅会关心下载速度，想必也会经常担心文件安全性和法律问题。平时大家不时会看到各种关于信息安全的新闻，又或者听说有留学生在国外使用迅雷等下载工具被警方带走等等。不说别的，我们每个人都有想要下载却不想被别人知道的时候。这个章节就是给大家系统地搞清楚几个问题：我在下载的时候，谁在看着我？谁又能看到我？有什么法律风险？

文件安全——篡改很容易，改完难发现

首先我们需要了解到一个很关键的事实：**HTTP 协议是明文传输数据的**。像我们第一章提到的那样，浏览器中打开的控制台（快捷键 Windows：F12；macOS：⌥Option-⌘Command-I）中你可以看到所有 http 请求的内容，包括请求头，请求内容，回应头，回应内容和请求的文件等。


Developer Tools - http://image.baidu.com/search/index?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl=2&nc=1&ie=utf-8&word=%E5%B0%8F%E9%94%81
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
View:
☐ Group by frame
☐ Preserve log
☐ Disable cache
☐ Offline
Online
Filter
☐ Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
2000 ms
4000 ms
6000 ms
8000 ms
10000 ms
12000 ms
14000 ms
16000 ms
18000 ms
20000 ms
22000 ms
24000 ms
26000 ms
28000 ms
30000 ms
32000 ms
34000 ms
36000 ms
Console
top
Filter
Default levels
中
12:08

Name	Status	Type	Initiator	Size	Time	Waterfall
index?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl=2&nc=1&ie=utf-8&word=%E5%B0%8F%E9%94%81	200	document	Other	236 KB	483 ms	
mod_6f6741d.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
co_b1eb78d.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	46 ms	
result_2109f7c.css	200	stylesheet	index?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl...	(from disk cache)	47 ms	
slider_ecce195.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	47 ms	
userInfo_5bd6198.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	48 ms	
logo-2X_b99594a.png	200	png	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
camera_new_off_a552294.png	200	png	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
AvFilterView_5709328.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	48 ms	
camera_new_on_4e3e250.png	200	png	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
mark_b68ff2e.png	200	png	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
uploading.gif	200	gif	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
base_a66ce51.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
cores_eabfeb1.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
AvMuiltSizeFilterView_5a57aa1.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	48 ms	
juicer_59c3d50.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
pageDisorderCheck_e040b58.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
pageDisorderTip_bf9f68d.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
AvTypeFilterView_cea6b92.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	48 ms	
pageCheckTool_f8aa598.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
result_a7dceb3.js	200	script	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from memory cache)	0 ms	
AvColorWallFilterView_cf8a646.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	48 ms	
AvColorFilterView_5b1da63.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	48 ms	
pageDisorderTip_42b50f0.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	49 ms	
loginbar_e8a6507.css	200	stylesheet	/search/index?tn=baiduimage&ps=1&ct=201326592&l...	(from disk cache)	49 ms	
alog.min.js?v=-17571-17571	200	script	index?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl...	(from disk cache)	19 ms	
data:image/png;base...	200	png	index?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl...	(from memory cache)	0 ms	
result-huge-bg_2c8c18f.png	200	png	base_a66ce51.js:3	(from memory cache)	0 ms	
panda_806dca6.png	200	png	base_a66ce51.js:3	(from memory cache)	0 ms	
panda_806dca6.png	200	png	base_a66ce51.js:4	(from memory cache)	0 ms	
loading_circle_40b82ef.gif	200	gif	base_a66ce51.js:3	(from memory cache)	0 ms	
data:image/jpeg;bas...	200	jpeg	base_a66ce51.js:3	(from memory cache)	0 ms	

113 requests | 270 KB transferred | Finish: 34.05 s | DOMContentLoaded: 794 ms | Load: 1.23 s

http 请求

我们在自己设备上看到这些没有多大问题，因为这些内容本来就是要给我们的。但是，一旦别有用心的人在服务器发送到客户端之前拦截到这些数据，那么他想要解读或者修改这些明文的数据将「易如反掌」。并且由于 HTTP 只通过状态码来确认请求状态，我们根本无法确定收到的数据是否已经被篡改。

这就是在计算机安全领域中大名鼎鼎的**中间人攻击**（MITM，Man-in-the-middle attack），这是我们通过 http 方式下载文件的时候最有机会碰到的一种攻击方式。

为了更好地理解文件下载中的中间人攻击，我们来举一个例子：

- 小明和小方是亲密的好朋友，他们俩都偷偷地暗恋同班

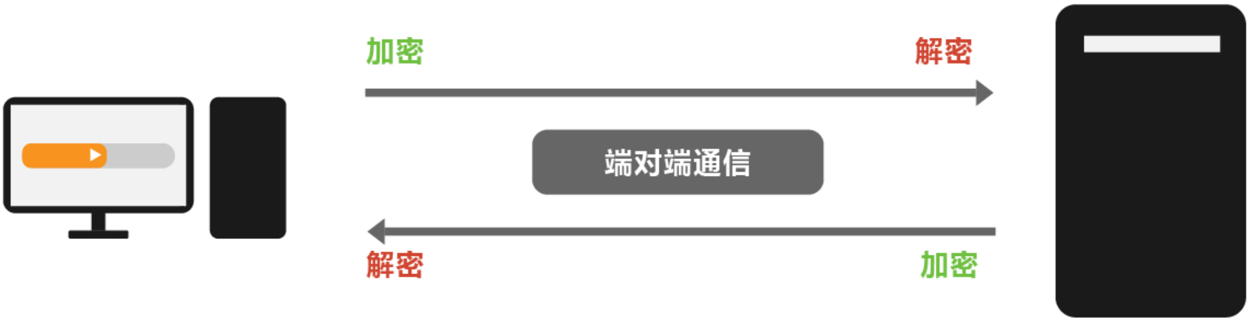
的小红。

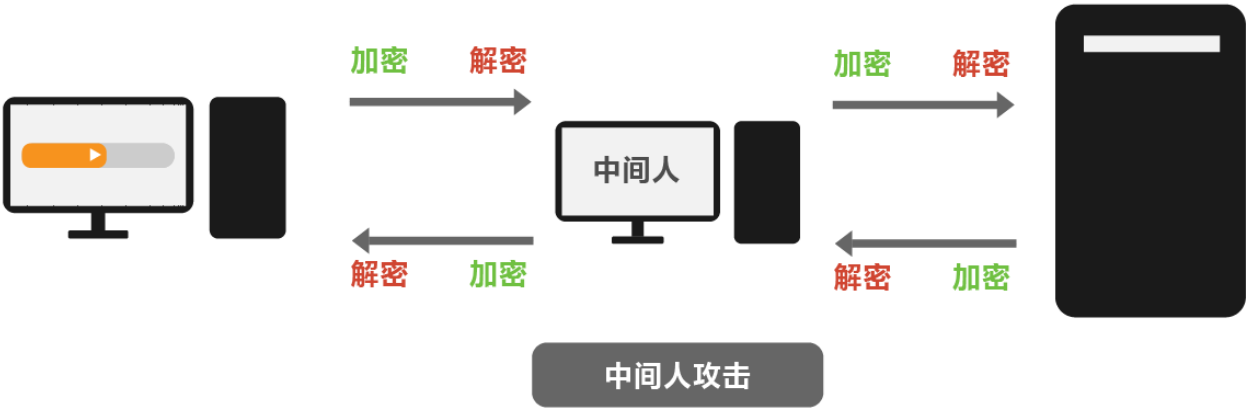
- 上课的时候小明经常和小红传纸条，可是他和她的座位相隔太远了，所以纸条从小明手里经过几个同学的传递才到小红的手中。

- 小方很想知道小明有没有趁机抢先向小红表白，又有没有说自己的坏话。所以小方编了个理由和一个传纸条的同学交换了座位。

- 接下来每次小明的纸条传到小方手里都会被他打开看一遍，然后把一些告白和打情骂俏的内容全都换成夸自己的话，小红传回来的纸条也是一样。

- 由于小明和小红之间平时羞于谈话，所以小方一直没有被发现。


加密
解密
端对端通信
解密
加密


加密
解密
加密
解密
中间人
解密
加密
解密
加密
中间人攻击

中间人攻击

在下载的情境中纸条即是我们要下载的文件，攻击者只需要让将我们需要下载的文件替换成他们准备好的文件即可。中间人攻击的难点在于如何加入到通信过程中（也就是偷到钥匙），中间人一般是这几个身份：

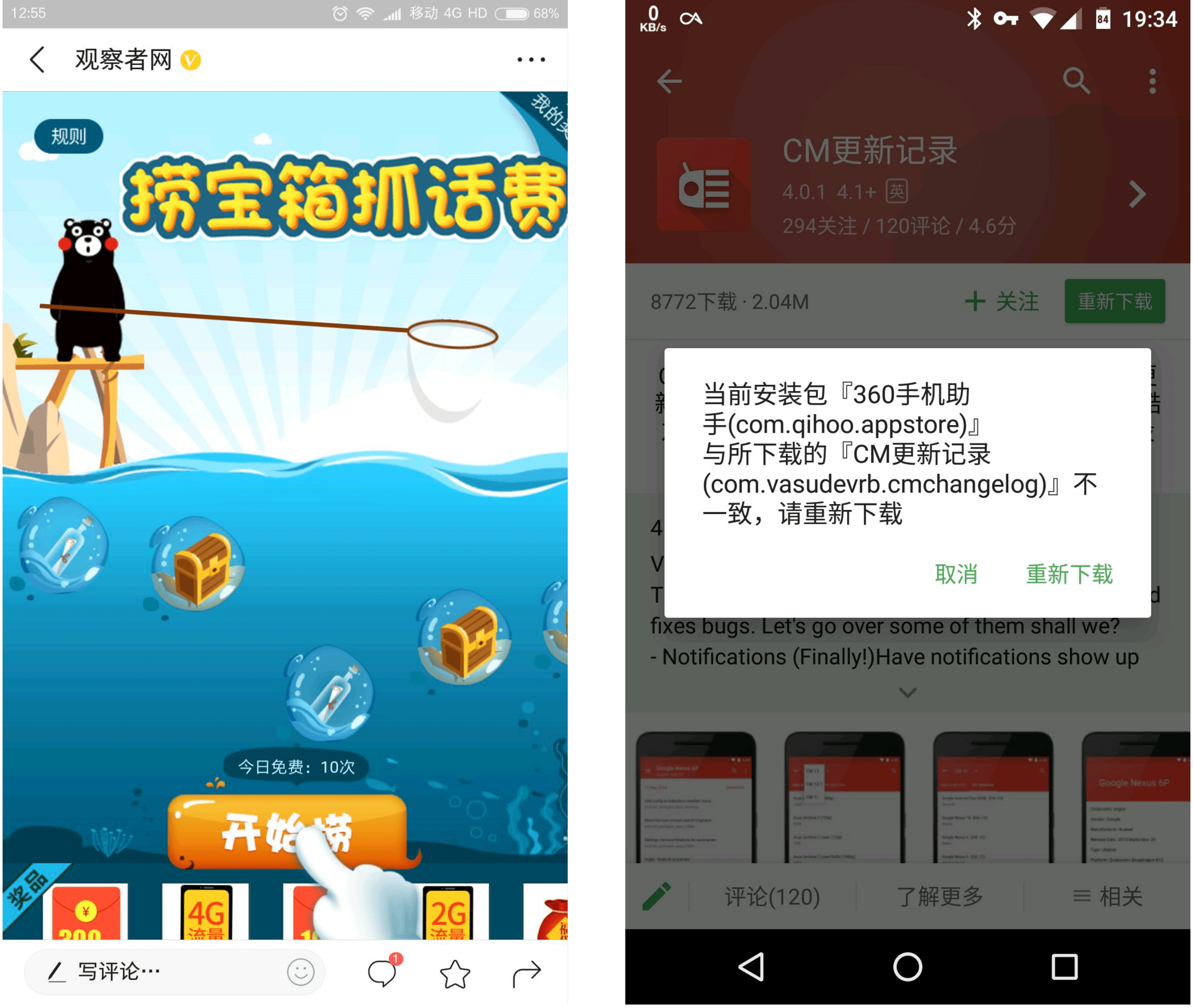
1. **连接到 Wi-Fi 等局域网中的其他设备**。这里分两种情况，一种是攻击者可以访问网关（路由器），比如「黑客」们经常在公共场合建立钓鱼 Wi-Fi，这种情况无需多说，「为所欲为」这个词可以说明一切，一切数据都可以被拦截。另外一种就是和你一样只是连接到同一个 Wi-Fi /局域网的设备，也可以发动中间人攻击（也被叫

做 ARP 攻击），详情可以看下面的自己动手尝试中间人攻击。

2. **流氓软件**。流氓软件和木马病毒一样，处于打击竞争对手和强行推广等目的，流氓软件直接在客户端篡改我们下载的文件。不同于木马病毒偷偷摸摸坏事的是，流氓软件需要用一个正当的理由掩饰这种行为。比如 3Q 大战的时候各家浏览器屏蔽或者篡改其他家软件的下载链接，浏览器就是下载器与服务器之间的那个「中间人」。

3. **硬件**。像是攻击者贴在 ATM 密码输入器上的复制硬件和插在网关上的数据监控器都是「中间人」。

4. **监守自盗**。平时我们使用某搜索引擎出来的网站经常先会瞬间跳转到一个地址再跳到我们想要访问的地址，然后你就会发现这个地址多了一些好像和网站本身风格好像不搭的广告（手机上更严重）；又或者你上着一个与运营商毫不相关的网站却弹出流量红包和流量球之类的推广，这个时候其实是某搜索引擎和这些运营商作为客户端和服务器的「中间人」劫持了你的请求。虽然不常见，不过这个时候它们是有能力篡改你的下载文件的，「监守自盗」这种中间人攻击最为防不胜防。


观察者网
规则
捞宝箱抓话费
今日免费：10次
开始捞
奖品
写评论…
CM更新记录
4.0.1 4.1+ 英
294关注 / 120评论 / 4.6分
8772下载 · 2.04M
关注
重新下载
取消
重新下载
评论(120)
了解更多
相关

当前安装包『360手机助手(com.qihoo.appstore)』与所下载的『CM更新记录(com.vasudevrb.cmchangelog)』不一致，请重新下载

fixes bugs. Let's go over some of them shall we?
- Notifications (Finally!)Have notifications show up

手机上的中间人攻击

FTP 与 HTTP 采用了相同的底层协议，同时 FTP 也是明文传输协议，所以 FTP 的安全性问题可以参考 HTTP。

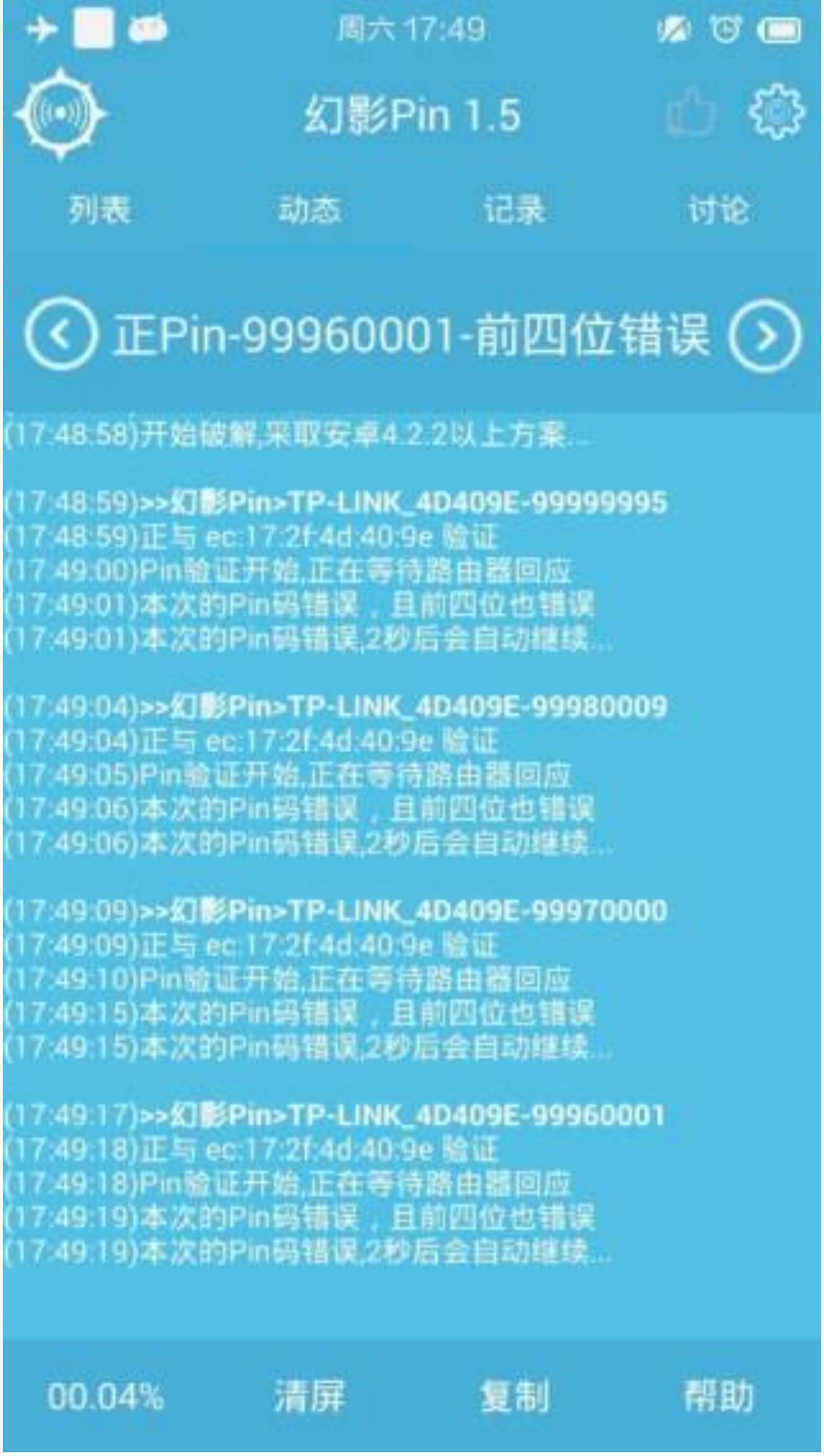
另外还有一种在各种公共场合很常见的攻击：**Wi-Fi 解除认证攻击（Wi-Fi deauthentication attack）**。它的原理就十分粗暴了，攻击者只需一个带有 Wi-Fi 的便宜开发板和一个移动电源即可。

我们平时连接或者断开 Wi-Fi 的时候设备都会发送一个数据

包来告诉路由器我要连接/断开了，攻击者就是利用这一点。当攻击者启动开发板上的攻击程序之后，攻击程序会持续向路由器和连接设备（例如手机）发送断开连接的请求，让设备无法连接到指定的 Wi-Fi，整个过程就是这么简单。

听起来好像危害不大，实际上攻击者可以：

> 在设备重新向路由器发送连接请求的时候拦截数据包，通过暴力破解（也就是根据装满密码的密码词典一个个尝试常见密码，更暴力的是把所有可能的密码都试一遍）的方式破解 Wi-Fi 密码。



```
(17:48:58)开始破解,采取安卓4.2.2以上方案...

(17:48:59)>>幻影Pin>TP-LINK_4D409E-99999995
(17:48:59)正与 ec:17:2f:4d:40:9e 验证
(17:49:00)Pin验证开始,正在等待路由器回应
(17:49:01)本次的Pin码错误，且前四位也错误
(17:49:01)本次的Pin码错误,2秒后会自动继续...

(17:49:04)>>幻影Pin>TP-LINK_4D409E-99980009
(17:49:04)正与 ec:17:2f:4d:40:9e 验证
(17:49:05)Pin验证开始,正在等待路由器回应
(17:49:06)本次的Pin码错误，且前四位也错误
(17:49:06)本次的Pin码错误,2秒后会自动继续...

(17:49:09)>>幻影Pin>TP-LINK_4D409E-99970000
(17:49:09)正与 ec:17:2f:4d:40:9e 验证
(17:49:10)Pin验证开始,正在等待路由器回应
(17:49:15)本次的Pin码错误，且前四位也错误
(17:49:15)本次的Pin码错误,2秒后会自动继续...

(17:49:17)>>幻影Pin>TP-LINK_4D409E-99960001
(17:49:18)正与 ec:17:2f:4d:40:9e 验证
(17:49:18)Pin验证开始,正在等待路由器回应
(17:49:19)本次的Pin码错误，且前四位也错误
(17:49:19)本次的Pin码错误,2秒后会自动继续...
```

幻影 Pin

让周围的无线设备例如监控摄像头，物联网设备失效。

在酒店会议等场合让所有 Wi-Fi 都无法被设备连接，只留下攻击者自己开的钓鱼热点。

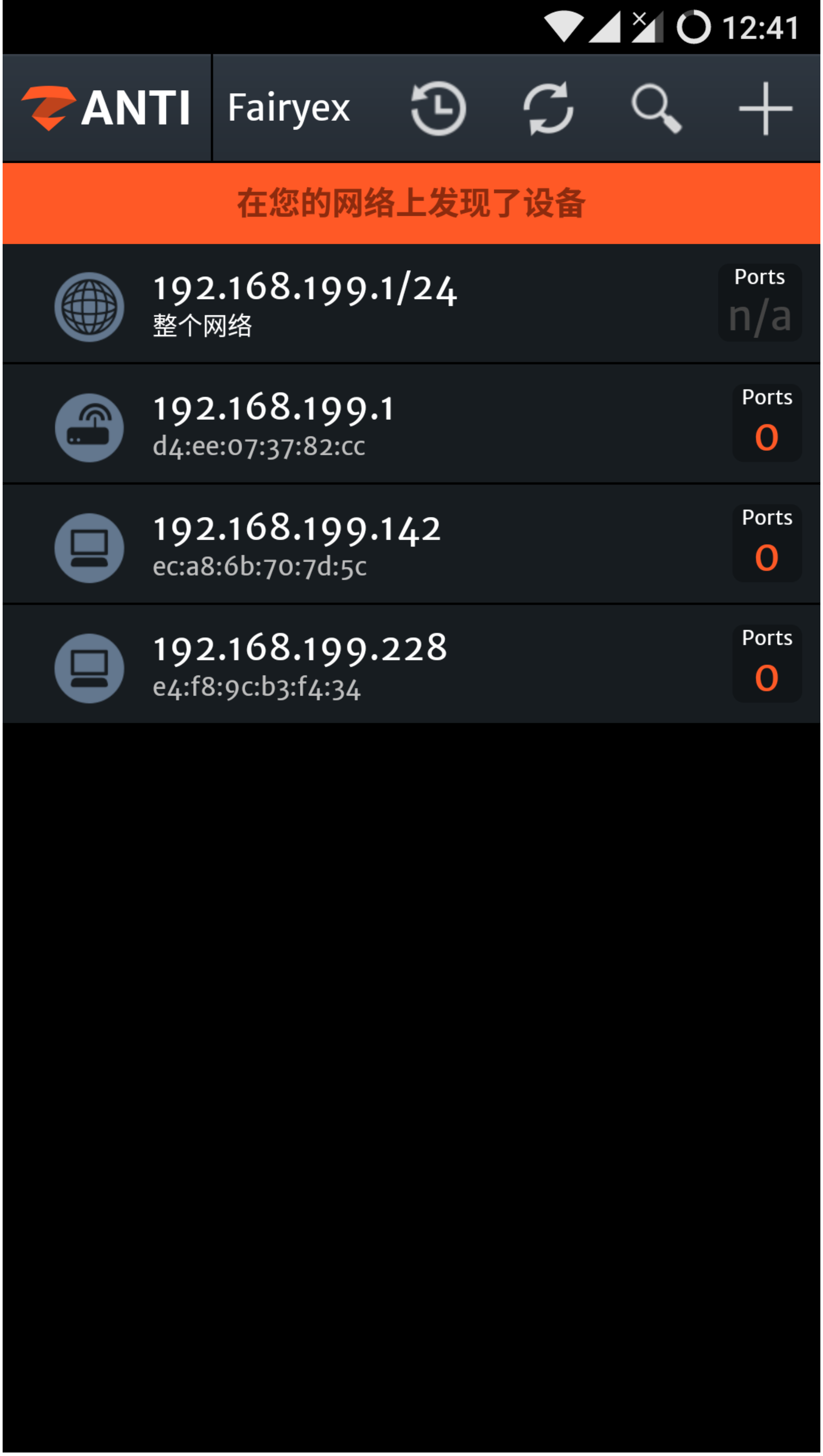
获得 Wi-Fi 密码后（例如饭店咖啡店等密码，或者按照第一条获取了密码），攻击者自己建立一个和原 Wi-Fi 相同 SSID（Wi-Fi 名字）和相同密码的钓鱼热点，然后攻击者迫使设备从原 Wi-Fi 断开后自动连接到钓鱼 Wi-Fi，接下来就是为所欲为的时间。

自己动手尝试中间人攻击

拦截与修改其他人的 HTTP 请求甚至篡改下载文件并不是多么难的一件事，甚至你自己就可以动手来试一下。

准备过程和工具十分简单，一点都不「黑客」。只需要安装一个 App —— Zimperium（曾经叫做 Zanti） 即可，难度跟一直点「下一步」安装一个软件差不多（仅限以下演示的功能，真要深入使用还是很「黑客」的，Zanti 甚至支持搭建钓鱼热点）。

打开 Zanti 同意使用协议之后，Zanti 会自动扫描当前 Wi-Fi 然后列出所有在这个 Wi-Fi 里面的设备。Zanti 只能告诉你每个设备的操作系统，可以搭配前面提到的显示设备型号的「Fing」App 确定你要开始攻击的设备。



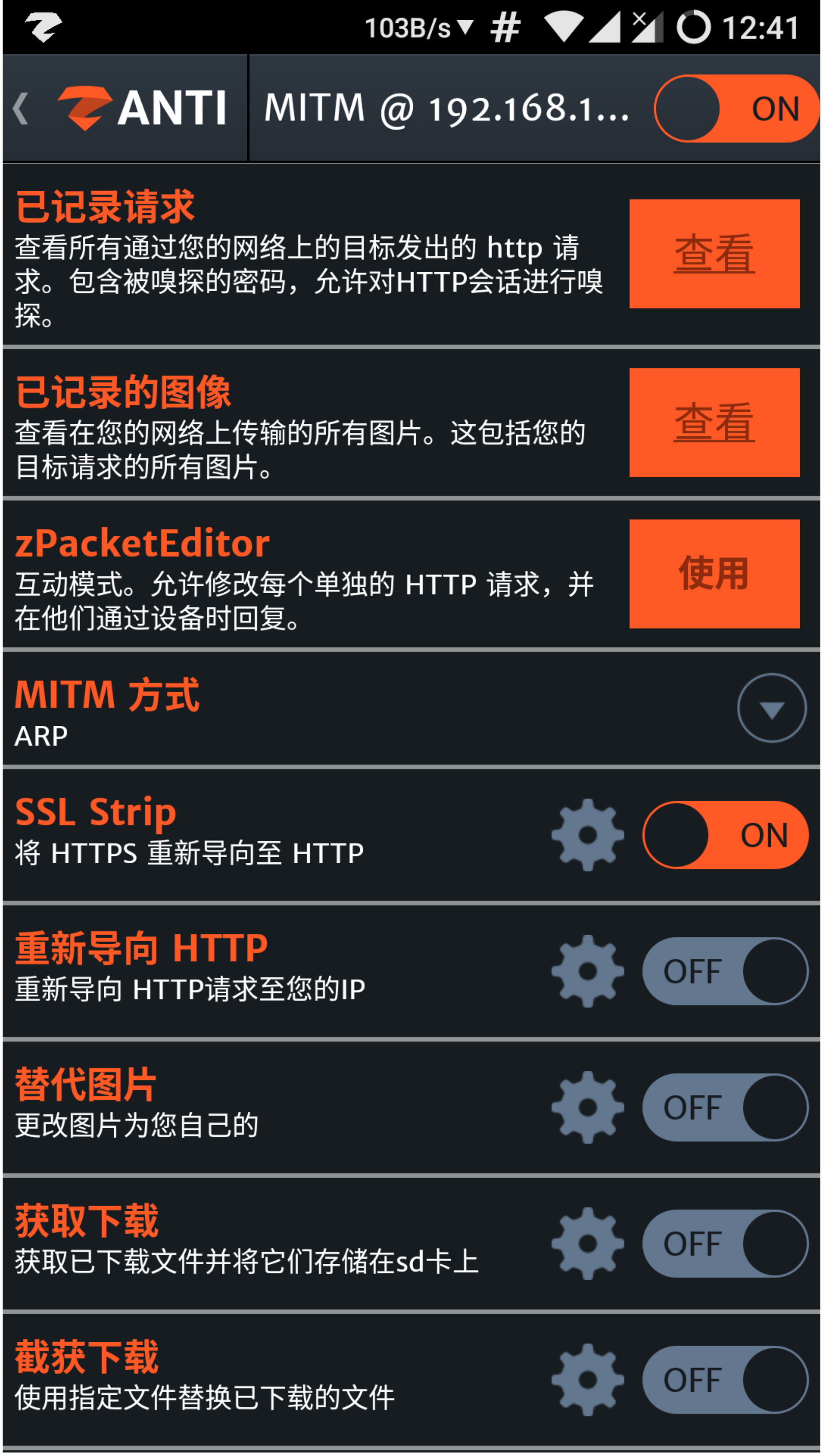
在您的网络上发现了设备

192.168.199.1/24 整个网络	Ports n/a
192.168.199.1 d4:ee:07:37:82:cc	Ports 0
192.168.199.142 ec:a8:6b:70:7d:5c	Ports 0
192.168.199.228 e4:f8:9c:b3:f4:34	Ports 0

Zimperium 界面

点击目标设备，接下来选择中间人，点击右上方的 OFF 打开中间人攻击。接下来你就可以使用列表里面的功能来对目标

设备做出各种操作了，是不是非常便捷简单？Zanti 不仅可以获取到目标设备所有的请求，图像。还能单独修改每一个请求，获取拦截下载文件，甚至插入自己的代码到网页中，这一切只需动动手指，不需要相关的知识。中间人攻击就是这样简单有效。



已记录请求
查看所有通过您的网络上的目标发出的 http 请求。包含被嗅探的密码，允许对HTTP会话进行嗅探。
查看

已记录的图像
查看在您的网络上传输的所有图片。这包括您的目标请求的所有图片。
查看

zPacketEditor
互动模式。允许修改每个单独的 HTTP 请求，并在他们通过设备时回复。
使用

MITM 方式
ARP

SSL Strip
将 HTTPS 重新导向至 HTTP
ON

重新导向 HTTP
重新导向 HTTP请求至您的IP
OFF

替代图片
更改图片为您自己的
OFF

获取下载
获取已下载文件并将它们存储在sd卡上
OFF

截获下载
使用指定文件替换已下载的文件
OFF

Zimperium 中间人攻击

谁在监控——全世界都有能力看见你

就在前面我们就说了「监守自盗」的问题，所有能篡改文件的方式都能用来监视。由于 HTTP 明文传输的特性，监控起来可以说是十分轻松。

在国家层面，中国有公共信息网络安全监察（也就是常说的「网监、网络警察」），美国有 FBI 与 NSA；其他国家除了相关部门，还有各种专门与各个运营商与公司合作的律师事务所。这些部门可以在法律与政府的支持下**合法地持续监控**所有 HTTP 上传下载流量。

简单说一下 FBI 与 NSA 对于互联网信息的分工，NSA（National Security Agency）是负责信息收集这个方面的，像是前几年斯诺登曝光公众信息泄露和猖獗一时的 WannaCry 勒索病毒都和 NSA 脱不了干系。由于间谍与犯罪信息在没有确认之前界限非常模糊，所以 NSA 可以说「什么都管」。不过普通的互联网犯罪（例如违规 BT 下载）大部分时间还是 FBI（Federal Bureau of Investigation）负责的，当然 CIA 这个吃瓜群众有时候也会打打酱油。

国内相关法律与规定：《互联网信息服务管理办法》第十四条。

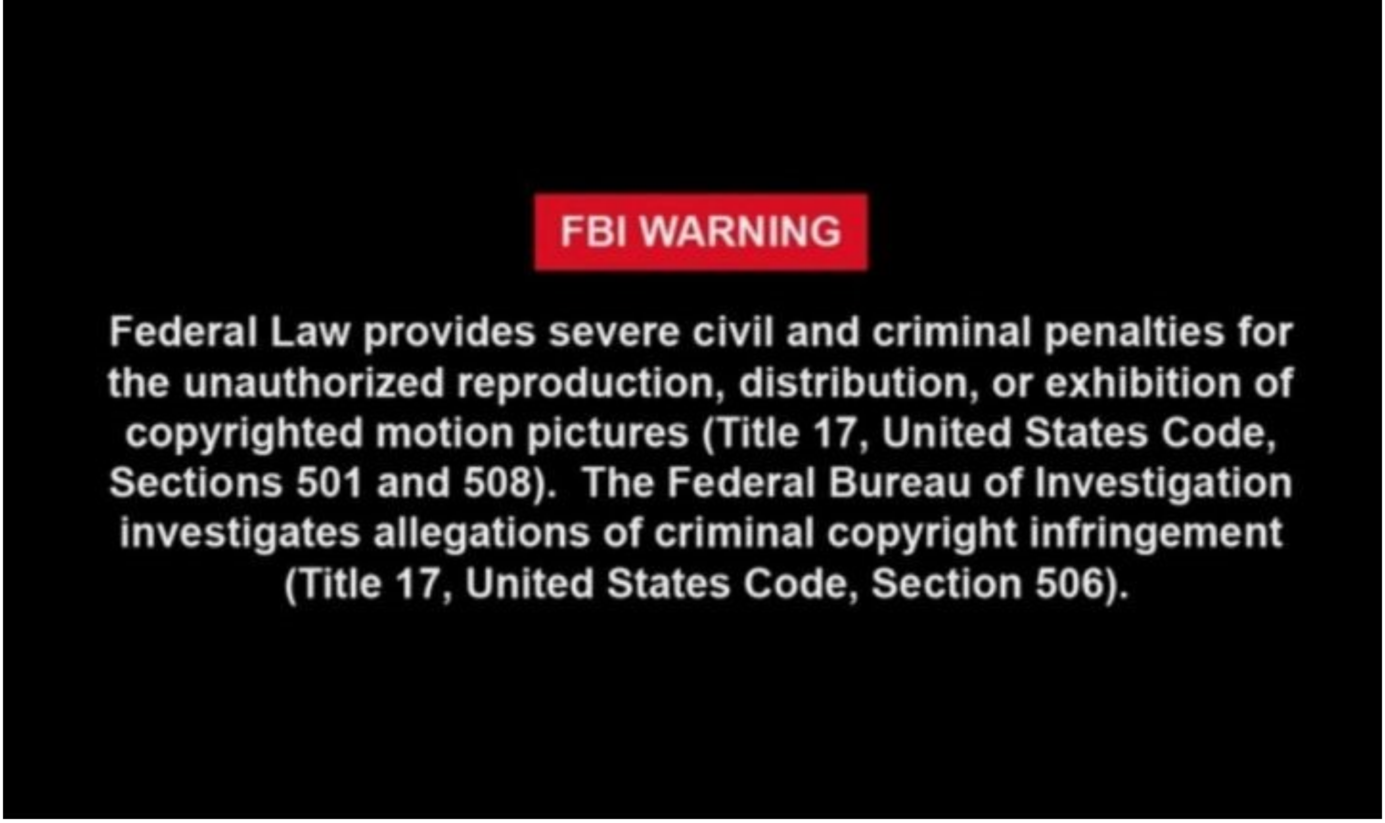
> 从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者，应当记录提供的信息内容及其发布时间、互联网地址或者域名；
>
> 互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。

> 互联网信息服务提供者和互联网接入服务提供者的记录备份应当**保存 60 日**，并在国家有关机关依法查询时，予以提供。

美国法律相关规定：

> Federal law provides severe civil and criminal penalties for the unauthorized reproduction,distribution ,or exhibition of copyrighted motion pictures (title 17,united states code,sections 501 and 508),the federal bureau of investigation investigates allegations of criminal copyright infringement (title 17,united states code,section 506)
>
> 根据联邦法律规定，凡对未经授权，而对受版权保护的电影作品进行复制、发行或公开展出者，可导致严厉的民事或刑事处分（美国联邦法典第 17 篇，第 501 条与 508 条）。美国联邦调查局负责调查侵犯版权的投诉 （美国联邦法典第 17 篇，第 506 条）。

上面就是大名鼎鼎的 FBI Warning，相信各位对它比对国内的法律更加熟悉吧。



FBI WARNING

Federal Law provides severe civil and criminal penalties for the unauthorized reproduction, distribution, or exhibition of copyrighted motion pictures (Title 17, United States Code, Sections 501 and 508). The Federal Bureau of Investigation investigates allegations of criminal copyright infringement (Title 17, United States Code, Section 506).

FBI Warning

在中国运营商层面，为了配合国家政策，所有网站主在使用网络运营商提供的网络服务或者主机运营商提供的云主机服务时都必须同意将数据公开透明地提供给网络监控部门。并且网站**自己的存储设备**上必须保存至少 2 个月的所有数据。这个执行力度非常足，像是直播网站甚至所有直播用户的录屏都必须保存 2 个月，下载记录啥的更不用说了。

在公共设施方面，例如：大学，公司，车站等。一般都可以看做一个大局域网，只需要在局域网出口处放置一个监控软件，局域网内所有的数据都跑不掉。特别是大学与公司这种需要进行人员网络行为管理的地方，一般来讲都会配置专用的网络行为管理软件，大家搜索「深信服、网路岗、WoekWin」等相关的网络行为管理软件就可以知道学校/公司的 IT 部门可以做到什么程度了。

公共设施监控这方面，国外与国内差不多，甚至国外要更为严重。具体到各个国家太复杂，这里就不细讲（我知道你们关心的是 BT 下载，请看下文），想要知道的留学生或者外国朋友可以在文章留下评论。

网路岗10能解决什么问题？

- 保护公司资料，如禁止U盘拷贝、备份邮件和打印输出资料等等
- 记录上班炒股、看视频、网购、炒私单等等不良行为
- 精准控制个人网络带宽，控制抢占带宽资源
- 记录常用的聊天内容、QQ文件传输等。
- 深度了解员工工作状态

谁在使用网路岗？

- 各类企业——控制上网行为，保护公司资料
- 政府单位——优化网络带宽，提高工作效率
- 公司网管——管理内部电脑设备、网络分析
- 大中小学——过滤上网，创建绿色校园网络

公共设施监控

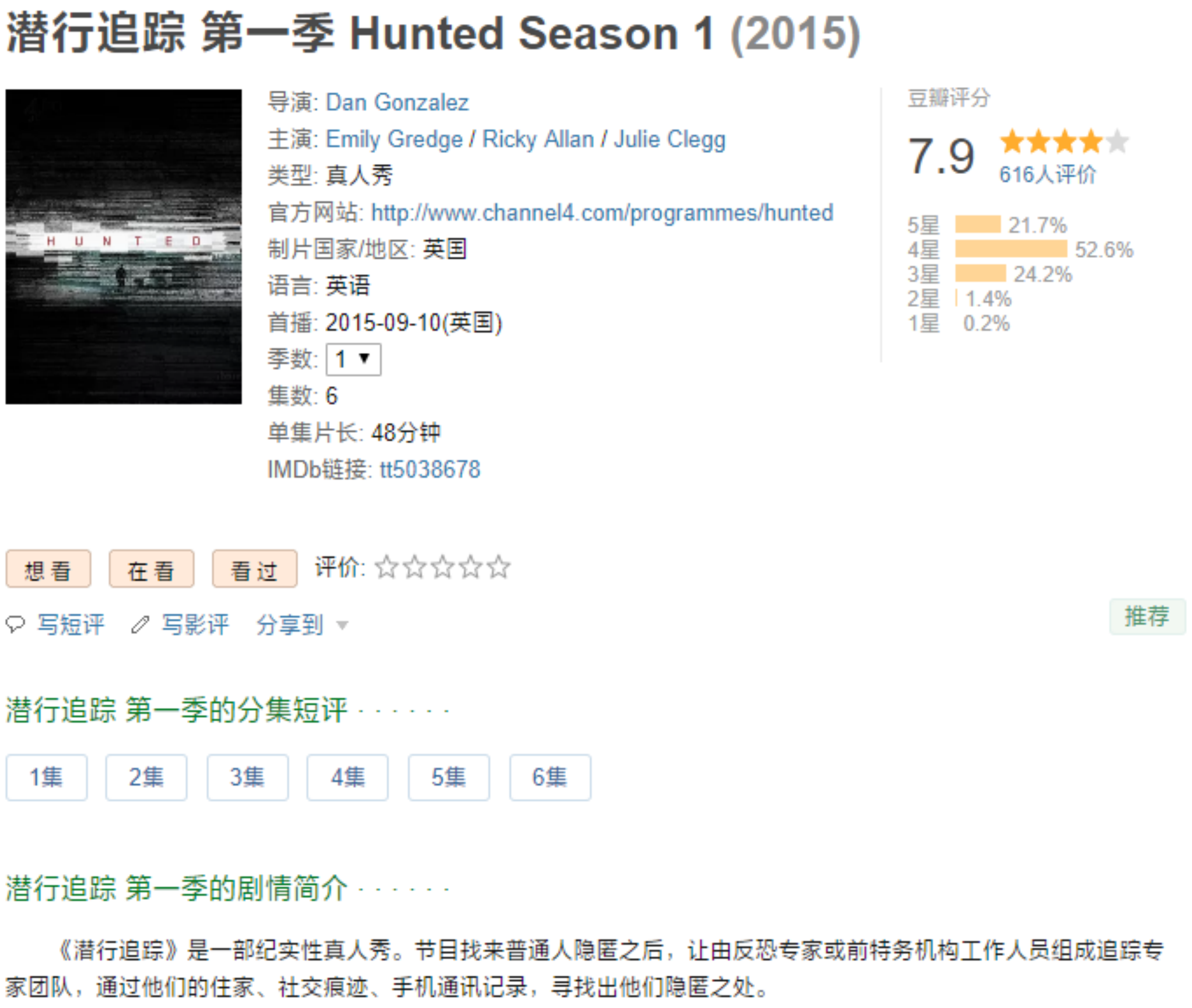
监控本身不是坏事，因为我们每时每刻都处于被监控的情景之下，监控可以更好地保证国家主权和个人的生命财产安全。侵犯隐私与否要看数据是否用于特例分析，如果这些最后会被匿名化用作大数据分析，对于个人来讲这些数据将毫无意义。

不过当你的数据被用于给你作用户画像且披露（泄露）给公

众的时候，披露（泄露）者就构成了严重的隐私犯罪，请尽情用一切能用的手段去维护自己的权益。

> 附：推荐大家一个关于国家监控的真人秀《潜行追踪》（英文：Hunted），有点猫鼠游戏的意思，这个真人秀挑选普通人作为「逃犯」，他们可以逃跑或者藏起来。然后由反恐专家、前情报机构调查人员、警察组成的专家猎人团队，模拟强力国家机构的监控手段与方式将他们找出来，如果在 28 天后「逃犯」都没有被「抓捕归案」，那么他们就会获得巨额赏金。

这个英国的真人秀节目被很多国家买了版权，特别是中国的版权被深圳卫视买了，以后可能还会有中国版。



潜行追踪 第一季 Hunted Season 1 (2015)

导演: Dan Gonzalez
主演: Emily Gredge / Ricky Allan / Julie Clegg
类型: 真人秀
官方网站: http://www.channel4.com/programmes/hunted
制片国家/地区: 英国
语言: 英语
首播: 2015-09-10(英国)
季数: 1
集数: 6
单集片长: 48分钟
IMDb链接: tt5038678

豆瓣评分
7.9 ★★★★☆
616人评价

5星	21.7%
4星	52.6%
3星	24.2%
2星	1.4%
1星	0.2%

评价: ☆☆☆☆☆

潜行追踪 第一季的分集短评 · · · · · ·

潜行追踪 第一季的剧情简介 · · · · · ·

《潜行追踪》是一部纪实性真人秀。节目找来普通人隐匿之后，让由反恐专家或前特务机构工作人员组成追踪专家团队，通过他们的住家、社交痕迹、手机通讯记录，寻找出他们隐匿之处。

潜行追踪

法律问题——主要看文件而不是方式

虽然前面监控问题说的十分严重，但是真正涉及到法律问题的却十分罕见。

一般来讲，现在能让你碰到法律问题的文件很难被 HTTP 下载到了，无论是国内还是国外。具体有哪些种类，国内可以参考《互联网信息服务管理办法》第十五条中的「九条底

线」：

互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)破坏国家宗教政策，宣扬邪教和封建迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)含有法律、行政法规禁止的其他内容的。

国内虽然有公共信息网络安全监察，但是面对庞大的互联网用户和法律的不完善，监控主要针对的还是与国家安全相关，上面九条里面就占了 6 条，版权就压根没有出现。这说明版权相关都不在重点打击之列（**不重点打击不代表不打击**）。对于以上九条类型的文件，有没有安全下载的办法

呢？唯一安全的办法就是**不下载（特别是前 6 条）**。

使用 HTTPS 下载链接

最近几年我们可以看到越来越多的网站的网址由 http:// 变成了 https://，这是因为 HTTP 的安全性已经满足不了公司和用户对于信息安全的需求，即使需要牺牲服务器性能也要做全局 HTTPS。那么 HTTPS 是什么？HTTPS 真的安全吗？这里就给大家讲解一下。

HTTPS 原理解释

我们还是以小明和小红的例子来讲解。在偶尔发现了小方的举动之后，小明准备下次传纸条的时候把内容转换一下，比如把所有的字母全部向后移动几位。可是想要小红看得明白，转换方法也需要写在纸条上传给小红，这样子小方不就也知道了吗?

经过一晚上的沉思，小明终于想到了一个超级棒的方法：

> 首先小明在把纸条发出去之前，先用 RSA 算法生成了两对数字。

RSA 算法的特性很有趣，举个简单的例子，我们能轻松算出 15287，27179 这两个不相等的质数乘积为 415485373，那么只给你一个 415485373 的时候你是几乎不可能得到这两个数字的（这个例子还比较容易算，当两个质数都是五六十位的时候普通电脑因式分解能算到宇宙毁灭）。

这个时候我们把 415485373 公开出去，这在密码学上叫做公钥；把（15287，27179）这对数字自己保管好，这在密码学上叫做私钥。（简略解释，非实际算法。）

这就是非对称加密算法的基本原理之一，它的两个特点就是：

- **知道公钥无法推测出私钥，知道私钥可以轻松推测出公钥。**

- 用公钥加公开的算法可以加密一条数据，但是你没法用公钥通过加密的数据逆向还原原来的数据，只能用私钥来解密。同理用私钥加公开的算法可以加密一条数据，但是你没法用私钥通过加密的数据逆向还原原来的数据，只能用公钥来解密。

这很像我们生活中常见的这种小防盗锁，任何人不用钥匙，按一下就可以轻松地把它锁上。但是如果要开锁就需要对应的钥匙才行。

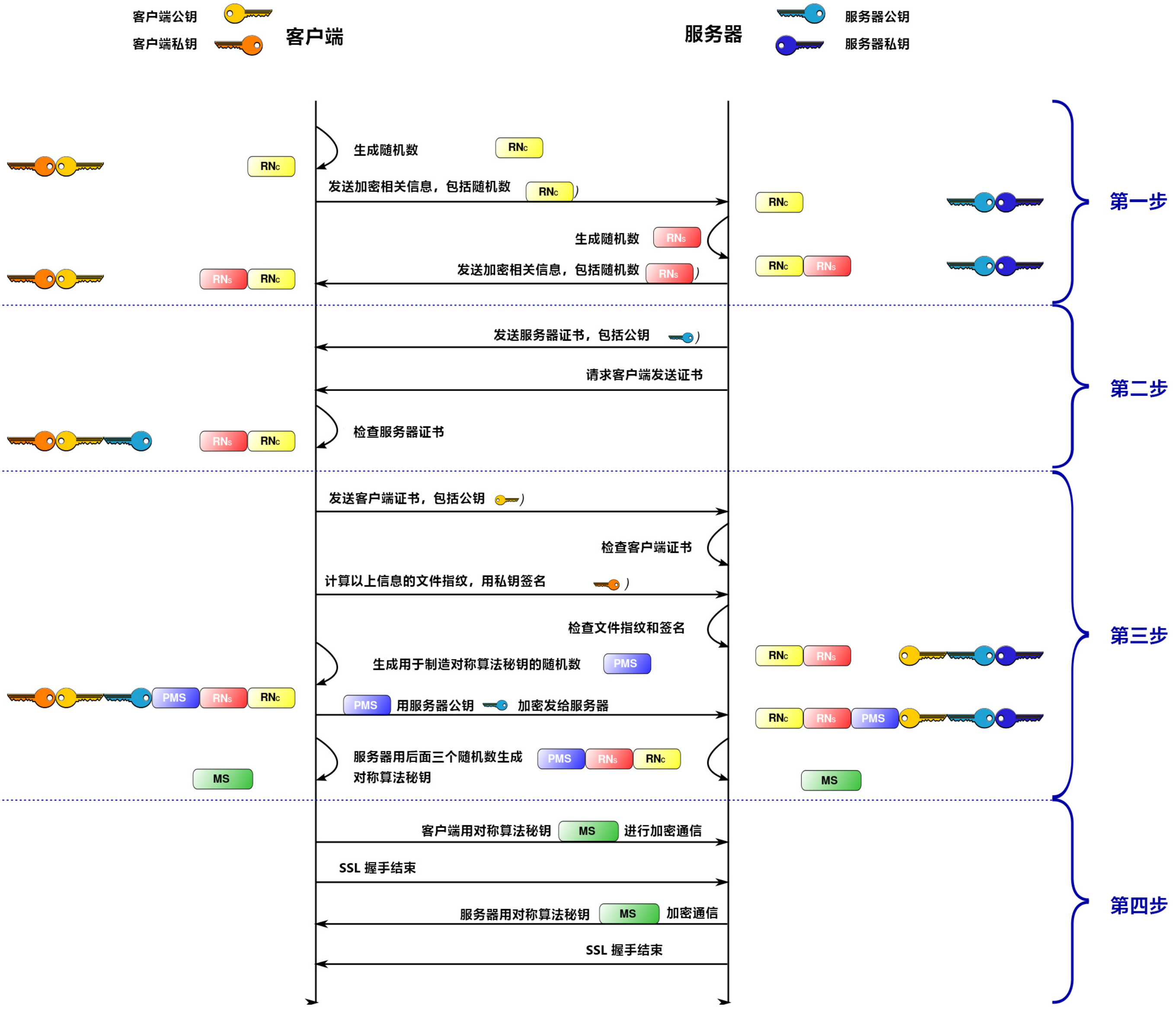
为了方便解释，下面我们把公钥称为公开数，私钥称为私密数。

- 小明先写一张纸条传给小红，内容是公开数和让小红想一个转换方法并且用 RSA 的公开算法加公开数加密这个转换方法。这时候小方拿到小明的纸条只能知道一个公开数和小明的小诡计。

- 小红在收到纸条后想了一个转换方法（比如字母全部向

后移动 3 位），然后把 RSA 的公开算法加公开数加密之后的转换方法写在纸条上传回给小明。这个时候小方手里只有公开数，无法知道这个转换方法是什么。

- 小明拿到了纸条之后，通过私密数解密就安全地拿到了转换方法，接下来小明和小红只需要用约定好的转换方法传纸条即可避免小方的窥探。


客户端公钥
客户端私钥
客户端
服务器
服务器公钥
服务器私钥
生成随机数
RNc
发送加密相关信息，包括随机数
RNc
生成随机数
RNs
发送加密相关信息，包括随机数
RNs
第一步
发送服务器证书，包括公钥
请求客户端发送证书
检查服务器证书
第二步
发送客户端证书，包括公钥
检查客户端证书
计算以上信息的文件指纹，用私钥签名
检查文件指纹和签名
生成用于制造对称算法秘钥的随机数
PMS
用服务器公钥
加密发给服务器
服务器用后面三个随机数生成
对称算法秘钥
MS
第三步
客户端用对称算法秘钥
进行加密通信
SSL 握手结束
服务器用对称算法秘钥
加密通信
SSL 握手结束
第四步

SSL 流程图，基于 @Essich 的原图翻译，遵守 CC 共享许可

首先，HTTPS 并不是一个新协议，它是普通 HTTP 上加了一层 S（SSL/TLS）层,这个层就是用来实现非对称加密算法

的。

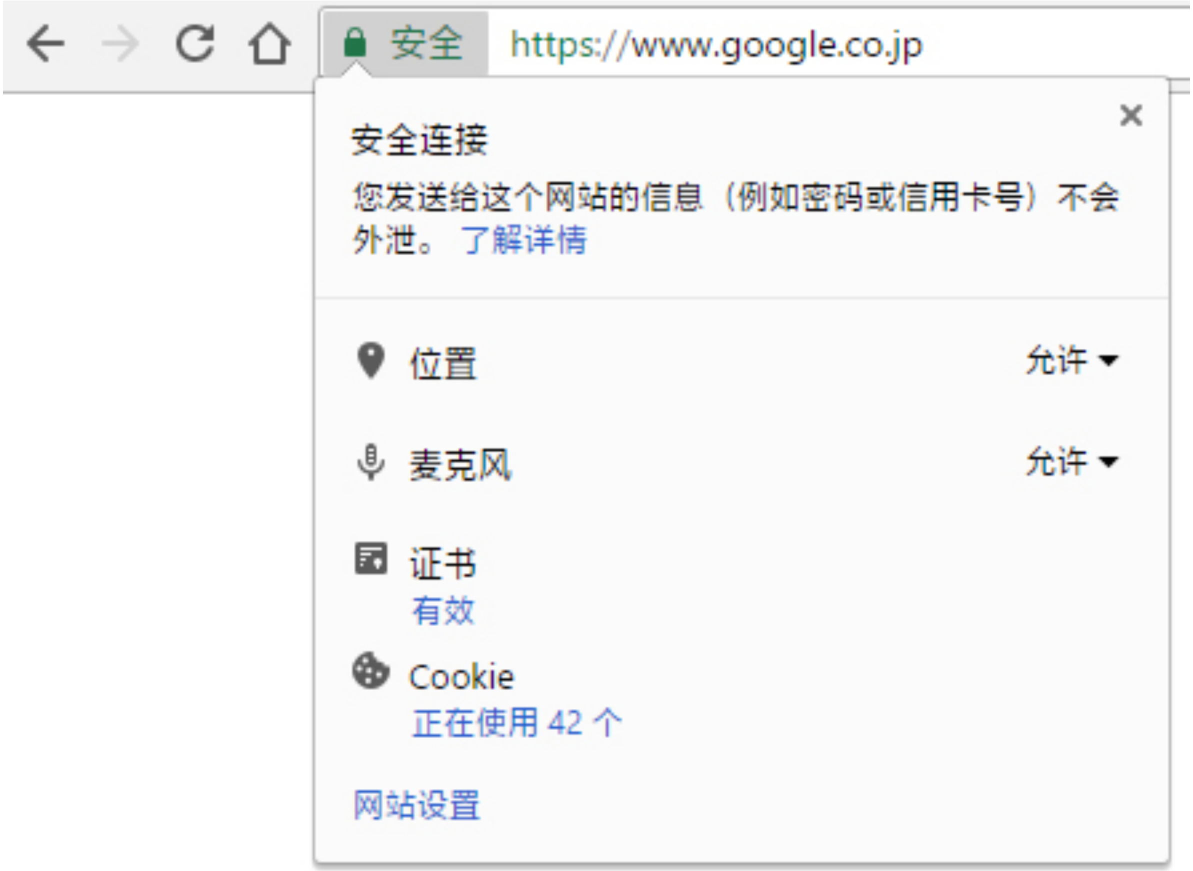
由于涉及大数运算，内容越多的情况下非对称加密算法在使用公钥/私钥进行加密/解密需要的性能和时间会成指数级上升，所以我们没办法对发送的数据本身进行非对称加密。一般来讲在 HTTPS 中使用非对称加密的只是文件指纹或者加密内容的**对称算法**（也就是一个钥匙既能加密也能解密的算法，就像小明和小红约定的转换方法）。

HTTPS 并不能完全保证安全

既然如此，HTTPS 就无懈可击了吗？并不是，小方只需要：

- 小明发出第一张纸条，小方把纸条拦截下来，然后把公开数换成自己用 RSA 生成的公开数 2。
- 小方再把纸条正常传递给小红，这时候小红认为纸条是小明发的，所以把用 RSA 的公开算法加公开数 2 加密之后的转换方法写在纸条上传回给小明。
- 小方拦截到小红的纸条，之后用自己的私密数 2 解密即可轻松拿到转换方法，接下来小方再用拦截到的小明的公开数加密小红的转换方法写在纸条上传递出去。
- 小明用自己的私密数成功解密获得转换方法，所以他对转换方法的保密性没有一丝怀疑。
- 之后小明和小红都认为自己纸条上经过转换的内容没人能看懂，殊不知小方已经掌握了他们的小秘密。

如此能击垮 HTTPS 安全体系严重的问题在设计的时候就被考虑到了，我们点击浏览器 HTTPS 网址旁边的小锁看到的证书就是为了解决这个问题而生的。



安全连接

您发送给这个网站的信息（例如密码或信用卡号）不会外泄。了解详情

位置 允许

麦克风 允许

证书
有效

Cookie
正在使用 42 个

网站设置

证书

解决这个问题很简单，只需要一个专门用来认证网站合法性的第三方组织，叫做 CA（Certificate Authority）。所有浏览器，服务器或者其他客户端都**内置**一份可信 CA 的公开数列表，所以小明和小红都有一份。小明用自己的公开数向 CA 申请一个证书通过后，「CA 机构信息+小明的信息+小明的公开数+证书的到期时间等」就构成了证书。为了防止证书被修改，CA 用可信 CA 列表中属于自己机构的公开数对应的私密数将证书的文件指纹加密生成一条证书签名。

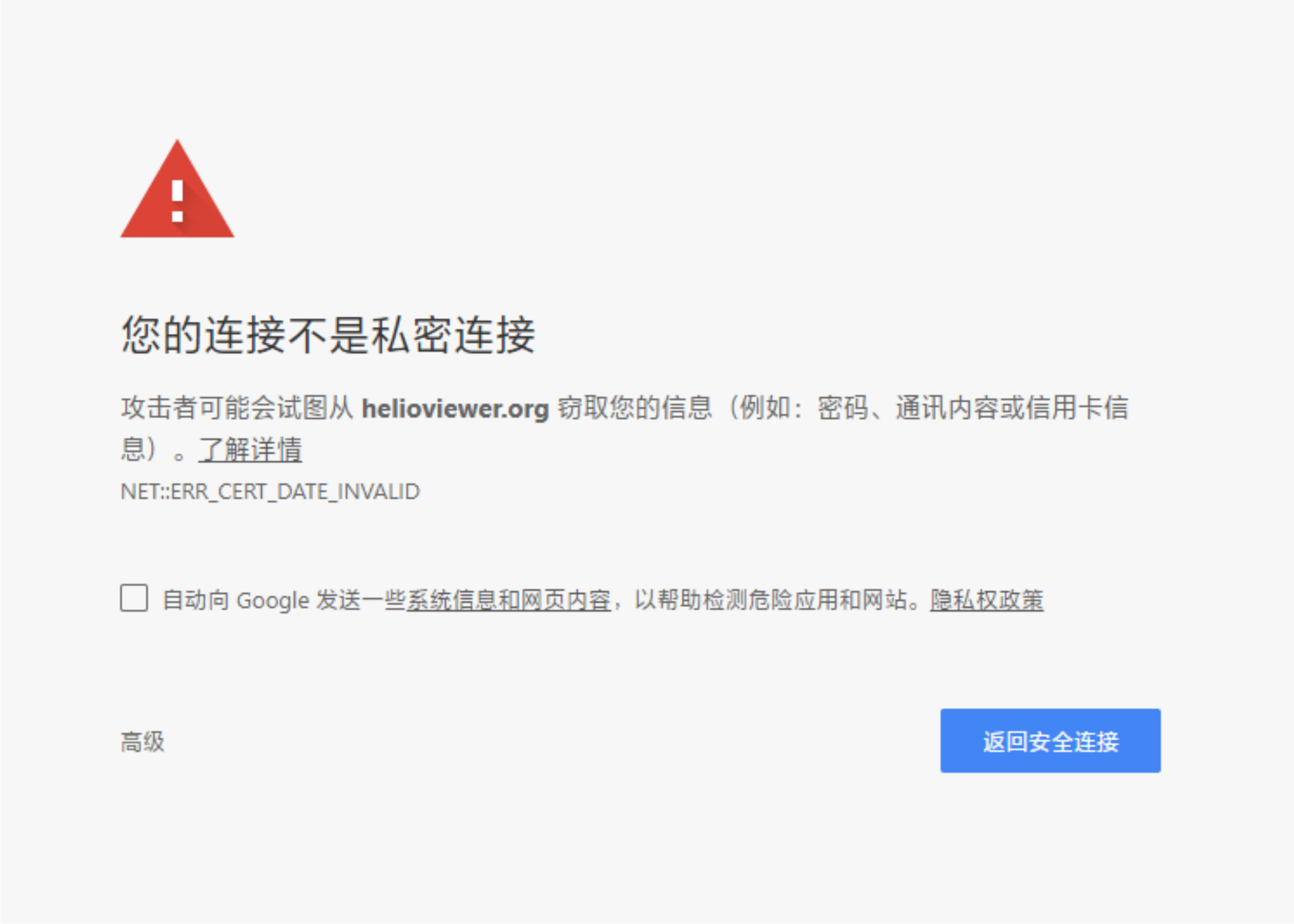
在上面的例子中，第一步小明将纸条内容，证书和证书签名都发给小红。

根据私密数加密的数据只可以用公开数解密，小红收到纸条后只需要：

- 用自己拥有的 CA 的公开数解密证书签名，如果得到证书的文件指纹即可证明这个文件指纹是由 CA 生成的（因为只有 CA 拥有自己机构的私密数）。
- 如果这个文件指纹和小明发过来的证书的文件指纹一样，即可证明这个证书内容是没有篡改过的 CA 颁发的证书。
- 根据证书里面小明信息可以确定证书是属于小明的，也就是里面的公开数是小明的公开数。

除非小方能够完美把直接伪装成小明骗过 CA，不然没有办法生成一个证明自己是小明的证书。所以小红可以安全地得到小明的公开数。

CA 就是靠信誉建立的，一旦有有一个证书被发现用于恶意用途那么这个 CA 分发的所有证书都会被视为危险的，所以 CA 只会给足够资质的申请者颁发证书。在现实中，证书是根据公司名字或者网站域名生成的，如果平时我们访问某些网站小锁会变成红色并且出现这个页面：



您的连接不是私密连接

攻击者可能会试图从 **helioviewer.org** 窃取您的信息（例如：密码、通讯内容或信用卡信息）。了解详情

NET::ERR_CERT_DATE_INVALID

☐ 自动向 Google 发送一些系统信息和网页内容，以帮助检测危险应用和网站。隐私权政策

网页警告

那么即是浏览器收到证书里面的身份信息和网站不匹配或者证书已经过期（上图）。至此，除开安全环节最弱的一环——用户作死之外，HTTP 安全性的坑已经被 HTTPS 填得差不多了。

传统 HTTP 与 FTP 如何保证一定程度的安全

不要连接未知 Wi-Fi

这个最常见的建议了，不过却非常有效。所有的技术防御手段都抵不过用户自己作死，所有免费的，公开的 Wi-Fi 热点

的安全隐患都是非常大的。即使 Wi-Fi 的所有者没有恶意，不怀好意的人也可以像上面那样对你发动中间人攻击。

如果你一定要连接公共的 Wi-Fi，请同时使用防御中间人攻击的软件，比如 Zanti 推荐使用的自家防护软件 —— zIPS。

不要随意安装 HTTPS 证书

虽然 HTTPS 并不是完全安全，不过比起 HTTP 来可是要好上太多，尽量使用 HTTPS 来下载文件。还有最重要的一点就是前面说过的所有技术防御手段都抵不过用户自己作死，HTTPS 也是如此，千万不要顶着红色小锁和感叹号继续浏览网站，或者因为蝇头小利和所谓的「为了确保安全/验证设备」的理由去安装来历不明的证书（安装证书即代表你把这个机构颁发的所有证书都纳入了信任列表）。

正规的网站绝对不会出现证书过期或者名称不符合的现象。

记得校验 MD5（也就是文件指纹）

许多网站或者下载提供者都会给自己的文件提供 MD5 码或者 MD5 文件，下载完成之后校对一下可以防止文件错误或者被篡改。

注意网速与 Wi-Fi 的异常变化

也许你在自己动手尝试中间人攻击的时候就已经发现了，被攻击的设备是可以感觉到网速明显变慢的，这是因为所有请

求都多了一层 Zanti 处理的步骤。平时我们在上网的时候如果突然感受到网速异常变慢，打开防御软件之后网速明显变快，那么可能在网络中有人正在监控你的设备。

同时也要警惕 Wi-Fi 无故断连和重连，如果出现这种情况，或者周围所有有没有密码的 Wi-Fi 都连不上，只剩下一个「CMCC」「ChinaNet」在那里诱惑着你。这个时候私人 Wi-Fi 请更换（隐藏） Wi-Fi 名称与密码，更换之后如果断连情况消失，那么很有可能在你附近有一个对你（的 Wi-Fi）不怀好意的[1]。在公共场合碰到这种情况请使用手机流量，同时确认周围有没有可疑的人或设备。

此外还有使用代理或者虚拟专用网络下载的方法，由于相关原因不适合在文中讨论。

eD2K 与 BT 的安全，监控和法律问题

文件安全

eD2K 钓鱼服务器

早先 ed2k 高速隐秘的优点让它成为下载各种资源的优先选择，大量的用户在上面分享了巨量的非版权资源。这引起了版权方们的注意，为了打击各种非版权资源分享，钓鱼（又称间谍）服务器出现了。

这些钓鱼服务器是由版权方设立的，它们的工作就是提供假的热门资源的 eD2K 文件链接，以此获得下载这些资源的用户信息，返回给这些下载者的则是空文件或者垃圾文件。

不过到现在这些钓鱼服务器也没剩下几个了（当然中国还有），只要更新 Emule 的安全服务器列表就可以很大程度上解决这个问题。

BT 下载的钓鱼文件

由于 BT 下载天生的特性，导致很难在下载的时候篡改下载的文件。于是恶意攻击者们就把重心转向了安全性最弱的环节——用户本身。

比如，当你下载一个文件之后却发现没有任何程序可以打开它，同时下载的还有一个名字叫做「请安装专用解码器打开文件」的 exe/vbs/bat 程序；把 exe 重命名为常见的播放器或软件名称；一个加密的 RAR，附上一个教你去某某网站获取密码的「解决方案」文本。比起这些来，下到葫芦娃已经是非常良心了。

这些都是常见的钓鱼手段，每天都会有不少的用户中招。

监控问题——毫秒级实时监控

中国

中国政府对于 BT Tracker 一直是处于严厉打击的状态，不断地关停 Tracker。不过只需要通过 BitCometTracker 等软件就能轻松搭建一个 Tracker，所以 Tracker 屡禁不止。

而且 BT 下载的时候同伴的 IP 是清晰可见的，想要监控十分容易。搭建一个钓鱼 Tracker 即可，就连我们自己也可以

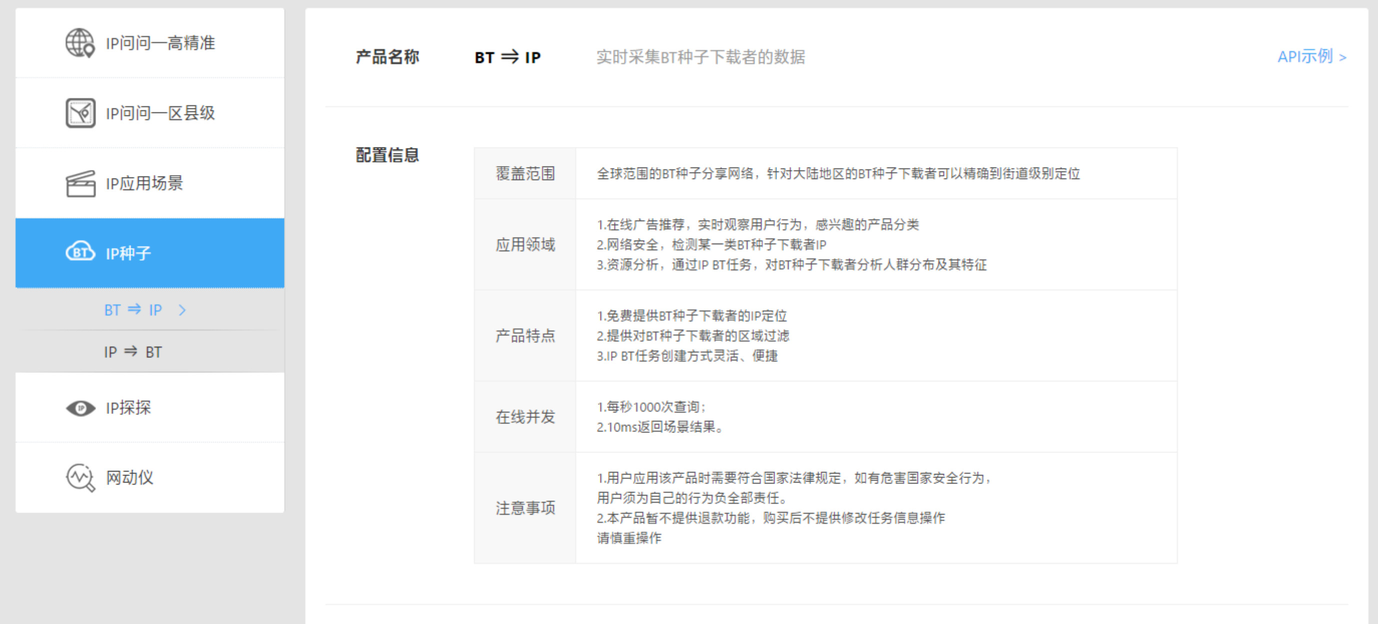
「追踪」一个下载者。运营商层面更简单，直接过滤出请求 Tracker 地址的请求就知道你在下载什么文件了。更别说自带文件评论和组队加速之类直接看到其他人账号的迅雷了。

想要知道的更具体？我们以 http://www.ipplus360.com/pros/bt/ 作为例子来看看吧。

由埃文+提供的各种 IP 服务里面就包括了关于 BT 下载监控的服务，不仅可以**实时**根据种子查找出**全球范围内**所有下载者的数据（IP 地址，现实地址），还可以根据 IP 找出**这个 IP 地址曾经下载过什么种子**。

埃文+还给相关部门提供了两个很现实的例子：

> 案例一： 我国某市安全部门，通过对若干带有敏感信息的种子，进行了多天的监控，最终锁定传播人的IP地址和地理位置。
>
> 案例二： 我国某省工信部门，通过对若干带有敏感信息的种子，进行了多天的监控，最终锁定传播人的IP地址和地理位置，并责令运营商对其网络监管加大力度。



产品名称 **BT ⇒ IP** 实时采集BT种子下载者的数据

配置信息

覆盖范围	全球范围的BT种子分享网络，针对大陆地区的BT种子下载者可以精确到街道级别定位
应用领域	1.在线广告推荐，实时观察用户行为，感兴趣的产品分类 2.网络安全，检测某一类BT种子下载者IP 3.资源分析，通过IP BT任务，对BT种子下载者分析人群分布及其特征
产品特点	1.免费提供BT种子下载者的IP定位 2.提供对BT种子下载者的区域过滤 3.IP BT任务创建方式灵活、便捷
在线并发	1.每秒1000次查询； 2.10ms返回场景结果。
注意事项	1.用户应用该产品时需要符合国家法律规定，如有危害国家安全行为，用户须为自己的行为负全部责任。 2.本产品暂不提供退款功能，购买后不提供修改任务信息操作请慎重操作

虽然实时根据种子查找出全球范围内所有下载者的数据的服务仅提供给政府部门，不过根据 IP 找出这个 IP 地址曾经下载过什么种子的服务可是人人都可以买，价格还不贵哦。

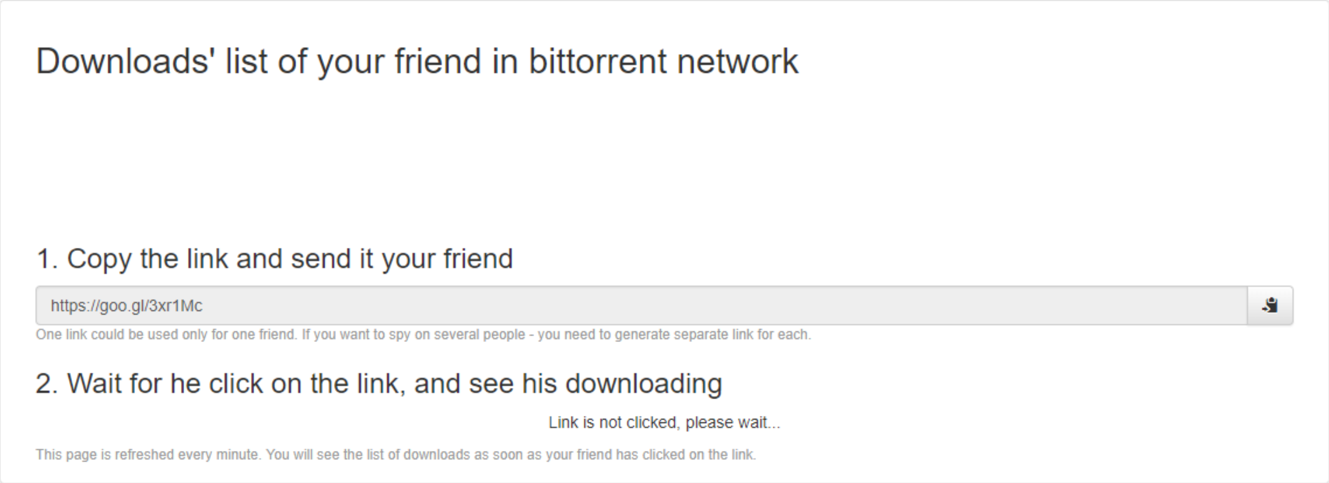
感兴趣的朋友可以继续看看埃文+的其他服务（当时 IP 探探和网动仪有点惊到我了），这还是民用商业级别而已，BT 下载的监控问题想必大家心里都有数了。

国外

既然国内都有商用级别的监控服务了，那么国外自然不用想。例如美国的 FBI 做的程度更加得细致，而且国外对版权资源和儿童色情资源打击力度十分之大。在大部分发达国家，只要手握版权的公司都会委托专门处理版权问题的律师事务所「版权巨魔」通过与网络运营商合作来帮助收集下载和提供资源的用户，等累积到一定数量时机成熟的时候再统一处理一波。

iknowwhatyoudownload 更是免费提供了根据 IP 地址查询最

近 BT 下载的文件功能，还有根据你提供的普通地址（例如 www.google.com）生成一条钓鱼链接，被点击后就能看到他最近下载的 BT 文件的「黑科技」。



Downloads' list of your friend in bittorrent network

1. Copy the link and send it your friend

https://goo.gl/3xr1Mc

One link could be used only for one friend. If you want to spy on several people - you need to generate separate link for each.

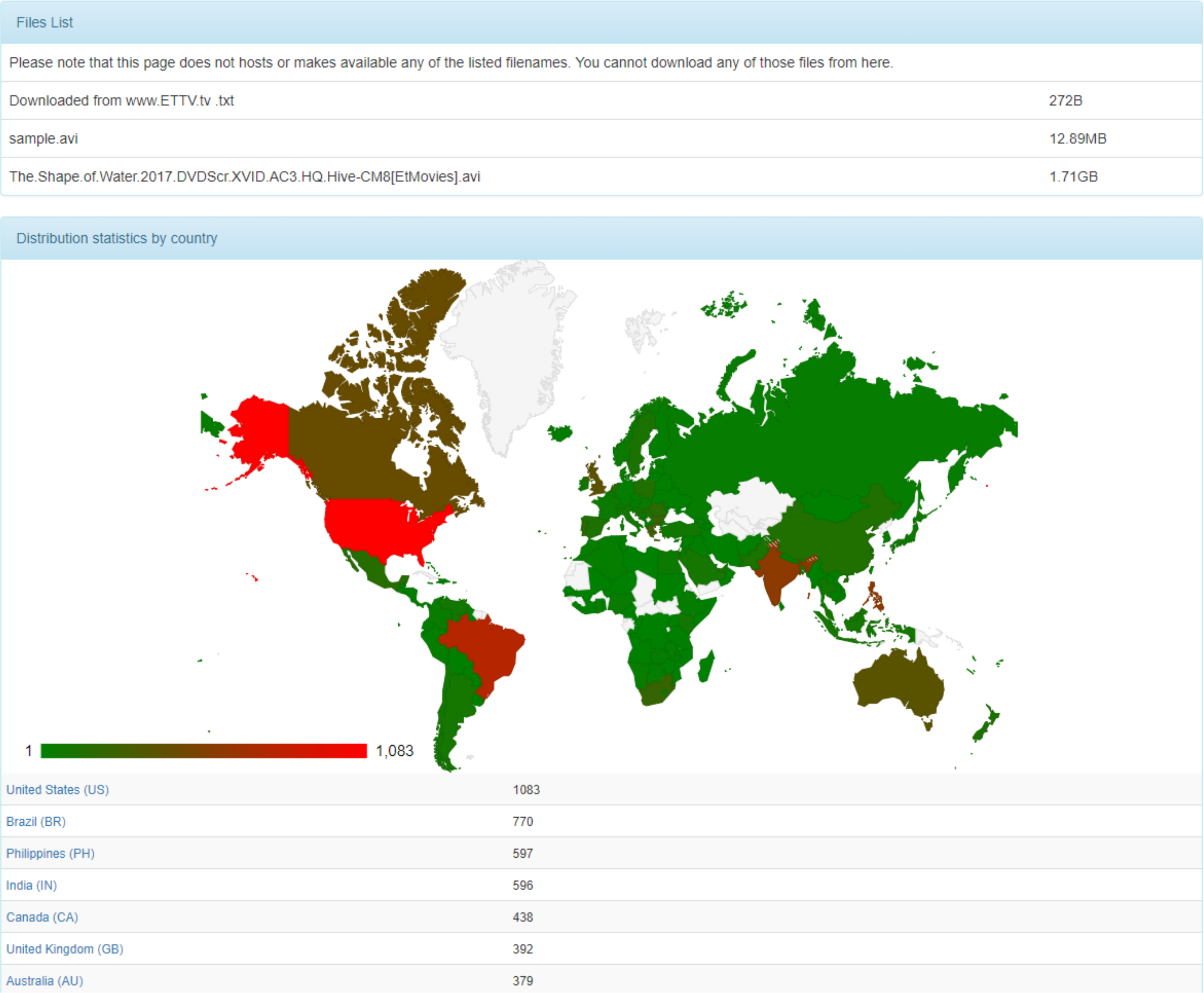
2. Wait for he click on the link, and see his downloading

Link is not clicked, please wait...

This page is refreshed every minute. You will see the list of downloads as soon as your friend has clicked on the link.

钓鱼链接

iknowwhatyoudownload 还免费提供全球热门数据，包括 BT 网络在线人数和最近热门的下载种子，甚至提供了每个文件的全球下载热力图。不过作为国外网站，它对墙内用户的统计就不那么精确了，在国外的朋友倒可以试一下。



Files List

Please note that this page does not hosts or makes available any of the listed filenames. You cannot download any of those files from here.

Downloaded from www.ETTV.tv .txt	272B
sample.avi	12.89MB
The.Shape.of.Water.2017.DVDScr.XVID.AC3.HQ.Hive-CM8[EtMovies].avi	1.71GB

Distribution statistics by country

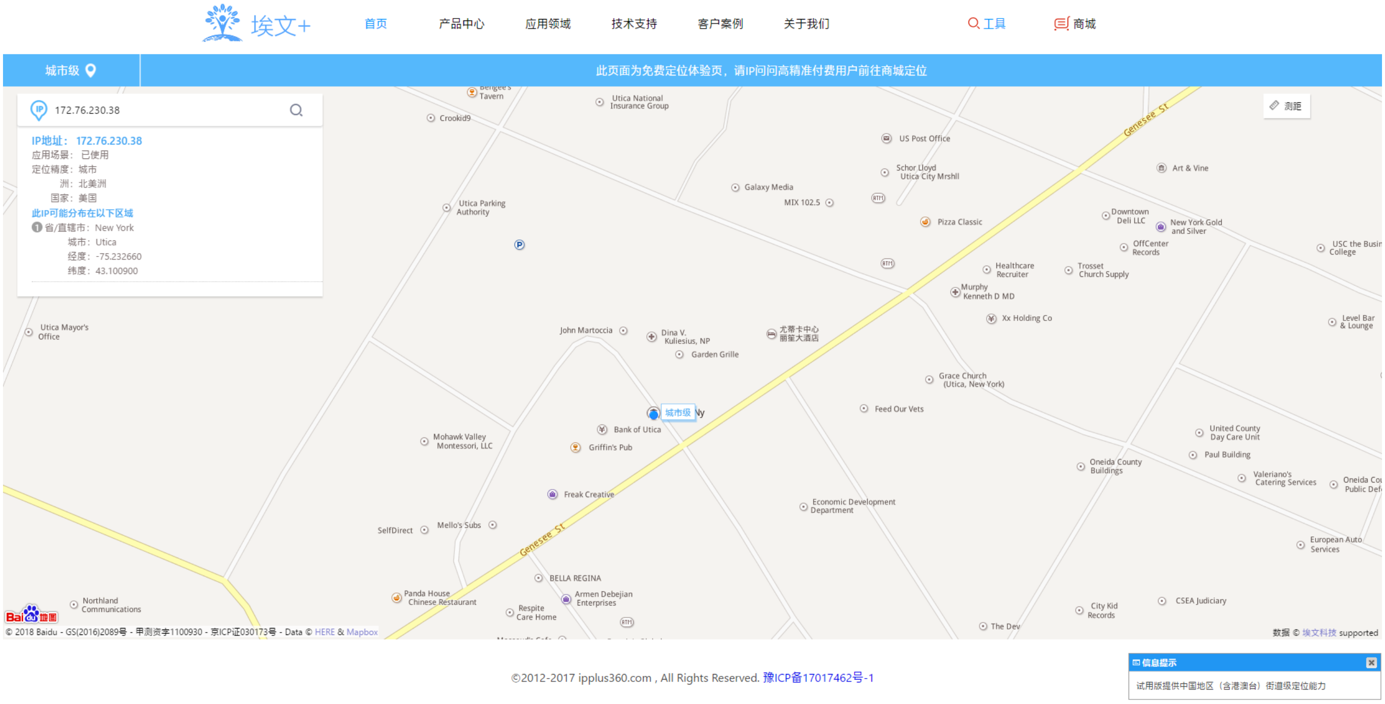
United States (US)	1083
Brazil (BR)	770
Philippines (PH)	597
India (IN)	596
Canada (CA)	438
United Kingdom (GB)	392
Australia (AU)	379

热力图

尝试自己追踪一个下载者

想要知道一个下载者在哪里并不难，一大堆 BT 下载工具都可以显示正在给你分享文件的小伙伴的 IP 地址。

拿到了 IP 地址之后使用一些 IP 地位服务即可拿到地址，比如国内的 IP 可以用埃文+提供的 http://www.ipplus360.com/ip/ 来查询，精确到街道还提供全景（由于我是美国 IP 所以展示不了）。其他诸如高德地图之类的也可以查询到。


埃文+
首页
产品中心
应用领域
技术支持
客户案例
关于我们
工具
商城
城市级
测距
Genesee St
Utica National Insurance Group
Crookid9
US Post Office
Art & Vine
Schor Lloyd Utica City Mrshll
Galaxy Media
MIX 102.5
Utica Parking Authority
Pizza Classic
Downtown Deli LLC
New York Gold and Silver
OffCenter Records
USC the Business College
Healthcare Recruiter
Trosset Church Supply
Murphy Kenneth D MD
Xx Holding Co
Level Bar & Lounge
Utica Mayor's Office
John Martoccia
Dina V. Kuliesius, NP
尤蒂卡中心丽笙大酒店
Garden Grille
Grace Church (Utica, New York)
Feed Our Vets
Bank of Utica
Griffin's Pub
Mohawk Valley Montessori, LLC
United County Day Care Unit
Paul Building
Oneida County Buildings
Valeriano's Catering Services
Freak Creative
Economic Development Department
SelfDirect
Mello's Subs
European Auto Services
BELLA REGINA
Panda House Chinese Restaurant
Armen Debejian Enterprises
Respite Care Home
Northland Communications
CSEA Judiciary
City Kid Records
The Dev
© 2018 Baidu - GS(2016)2089号 - 甲测资字1100930 - 京ICP证030173号 - Data © HERE & Mapbox
数据 © 埃文科技 supported

此页面为免费定位体验页，请IP问问高精准付费用户前往商城定位

172.76.230.38

IP地址： 172.76.230.38
应用场景： 已使用
定位精度： 城市
洲： 北美洲
国家： 美国
此IP可能分布在以下区域
❶ 省/直辖市： New York
城市： Utica
经度： -75.232660
纬度： 43.100900

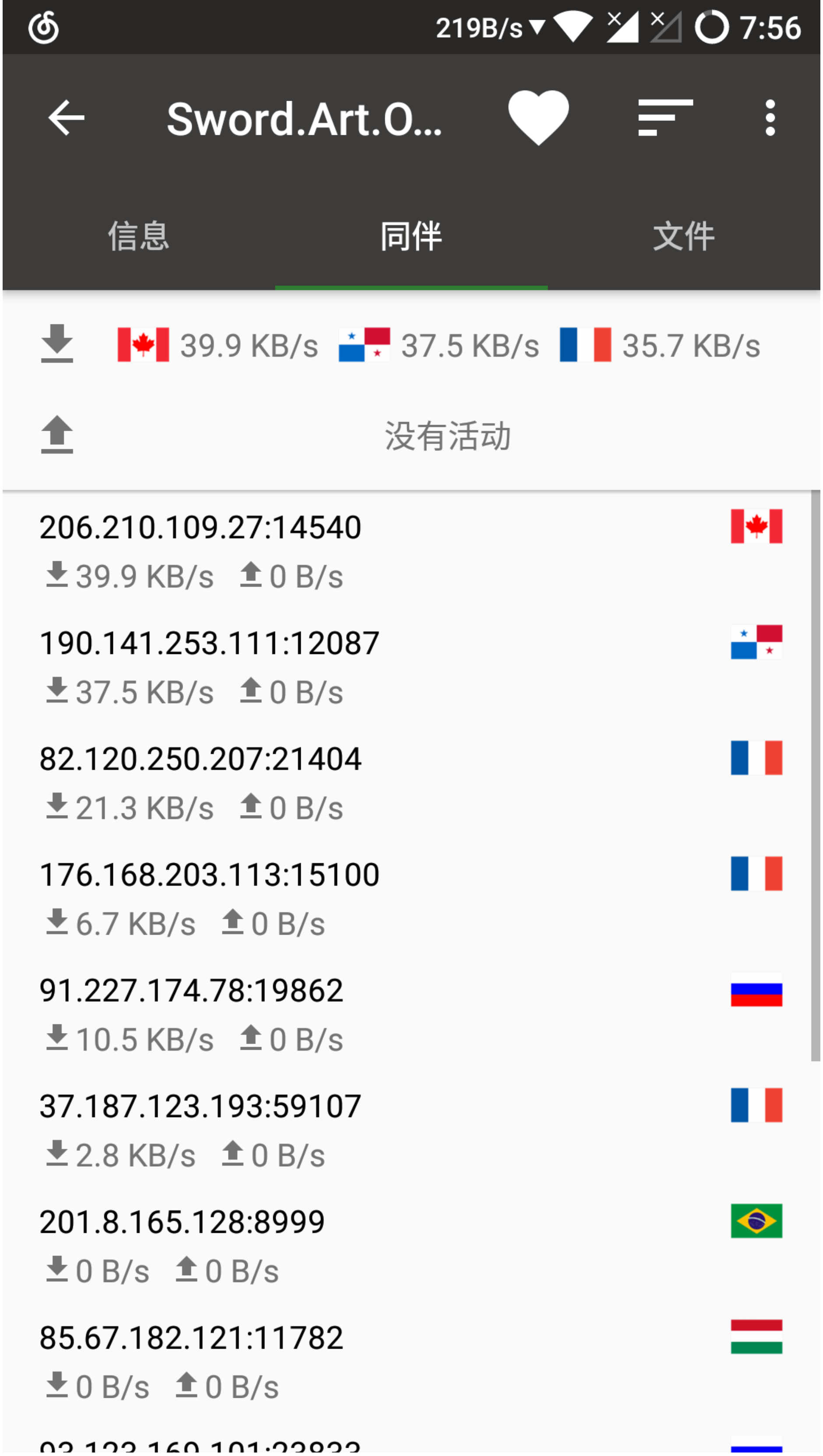
©2012-2017 ipplus360.com , All Rights Reserved. 豫ICP备17017462号-1

信息提示

试用版提供中国地区（含港澳台）街道级定位能力

法律问题——大部分是上传的锅

之前在科普的时候说过，BT 下载是可以用于很多用途的，像是游戏更新或者用于公开研究和学习的大量数据交换。所以 BT 下载很难也不能被封杀，像是我们会觉得国外特别是美国对 BT 下载会管得特别严格，动不动就特警破门啥的，其实没有那么严重。平时我们下载也是能看到很多外国小伙伴的，像是最近我下载的时候就看到了以下国家的朋友：



39.9 KB/s 37.5 KB/s 35.7 KB/s

没有活动

206.210.109.27:14540
39.9 KB/s 0 B/s

190.141.253.111:12087
37.5 KB/s 0 B/s

82.120.250.207:21404
21.3 KB/s 0 B/s

176.168.203.113:15100
6.7 KB/s 0 B/s

91.227.174.78:19862
10.5 KB/s 0 B/s

37.187.123.193:59107
2.8 KB/s 0 B/s

201.8.165.128:8999
0 B/s 0 B/s

85.67.182.121:11782
0 B/s 0 B/s

国内法律对 BT 并没有做出严格的规定，只有《中华人民共和国刑法》第二百一十七条有点关联。

> 以营利为目的，有下列侵犯著作权情形之一，违法所得数

> 额较大或者有其他严重情节的，处三年以下有期徒刑或者拘役，并处或者单处罚金；违法所得数额巨大或者有其他特别严重情节的，处三年以上七年以下有期徒刑，并处罚金：
>
> (一)未经著作权人许可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品的；
>
> (二)出版他人享有专有出版权的图书的；
>
> (三)未经录音录像制作者许可，复制发行其制作的录音录像的；
>
> (四)制作、出售假冒他人署名的美术作品的。
>
> 根据本条的理解与适用，通过信息网络向公众传播他人文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品的行为，应当视为「复制发行」。
>
> 还有制作、复制、出版、贩卖、传播淫秽物品牟利罪。

无论国内外都要抓住一个关键字——**复制发行**，即使是在美国，如果你只是下载而没有上传数据就不会构成复制。运营商也是重点打击上传流量而不是下载流量，只要你遵守下面几条建议，即使身在国外也能安全地享受 BT 下载的便利。

eD2K 与 BT 下载正版资源时保护自己的权利

最安全的就是使用 BT 做它该做的事情，例如下载开源系统或者非版权资源。下面的建议更偏向于在国外下载**正版资源**时保证安全。**国内个人下载只要不触及几条底线，不担心监控问题基本没有法律问题。**

不要在公共网络使用，在私人网络下载

无论是在国内外，学校与公司这种地方最好不要使用 BT 下载。特别是在国外，像是日本或者美国，这些国家对学校公司的对外流量控制特别严格，加上 BT「边上传边下载」的特性很容易给自己惹上警察。相比而言私人住宅就安全许多，毕竟国外私人领域的权限很高，很多美国人本身也在家用这些方式下载。

不要大流量

大部分运营商其实不会浪费资源去一个个去检测用户下载了什么，只有当某个用户的 BT 下载/上传流量异常才会检查你是否下了不能下的文件然后警告+断网，如果多次被运营商警告你的个人信息是有可能被提交到版权方手里面的。

尽量限制上传流量

相比下载流量，运营商对 BT 上传流量检测更为严格，而且一旦你在下载的时候有上传的行为即是触犯了法律。可能会面临罚款等惩罚（被版权公司委托的律师事务所会根据运营商提供的信息对所有触犯法律的用户发起共同诉讼。）

不过限制上传流量之后下载速度会变慢，因为 BT 协议会根据上传速度来分配下载速度。还有一个很难注意的点是许多视频网站（特别是国外朋友用代理上中国视频网站的时候）的客户端都会默认开启 P2P 来缓解服务器压力，请使用这些客户端之前注意相关的事项。

此外还有使用代理或者虚拟专用网络下载，和避免在头 60 天下载资源，尽量下载非本国资源两种方法。由于相关原因不适合在文中讨论。

磁力链接安全，监控和法律问题

我们平时使用迅雷下载磁力链接，有时候会发现最后还是会下载一个种子文件。理论上磁力链接不需要 Tracker 也可以实现下载任意文件，但是国内很多网站只是为了规避法律风险直接把种子文件转换成磁力链接，实际上我们是先通过 P2P 下载种子再通过种子下载文件。

这种情况下的确可以保证种子的存活率，不过剩下就相当于传统的 BT 下载了。只有真正的通过 DHT 网络获取数据的下载才可以避免监控问题。

最后我解答一个终极问题，有没有百分百安全，不会受到监控的方式去下载文件呢？答案是百分百没有，不过还是有几种方法可以无限接近这个目标，很可惜这些方法是**绝对不能出现在文章中的**（大家都懂，我也只能说到这里了）。